Common divisors of $a^n - 1$ and $b^n - 1$ over function fields

Joseph H. Silverman

Abstract. Ailon and Rudnick have shown that if $a, b \in \mathbb{C}[T]$ are multiplicatively independent polynomials, then $\deg\bigl(\gcd(a^n - 1, b^n - 1)\bigr)$ is bounded for all $n \ge 1$. We show that if instead $a, b \in \mathbb{F}[T]$ for a finite field $\mathbb{F}$ of characteristic p, then $\deg\bigl(\gcd(a^n - 1, b^n - 1)\bigr)$ is larger than Cn for a constant $C = C(a, b) > 0$ and for infinitely many n, even if n is restricted in various reasonable ways (e.g., $p \nmid n$).

Contents

Introduction

Let a and b be positive integers that are multiplicatively independent in $\mathbb{Q}^*$ and let $\epsilon > 0$. Bugeaud, Corvaja, and Zannier [2] recently showed that there is an $n_0 = n_0(a, b, \epsilon)$ so that

$$\gcd(a^n - 1, b^n - 1) \le 2^{\epsilon n} \qquad \text{for all } n \ge n_0. \tag{1}$$

In other words, $a^n - 1$ and $b^n - 1$ cannot share a common factor of significant size. Although elementary to state, the proof requires deep tools from Diophantine analysis, specifically Schmidt's subspace theorem [4].

Ailon and Rudnick [1] consider the analogous problem in which a and b are taken to be polynomials in $\mathbb{C}[T]$. They prove the stronger result

$$\deg\bigl(\gcd(a^n - 1, b^n - 1)\bigr) \le C(a, b) \qquad \text{for all } n \ge 1. \tag{2}$$

Mathematics Subject Classification. 11T55; 11R58; 11D61.
Key words and phrases. greatest common divisor, function field.

It is natural to consider the situation when a and b are polynomials in $\mathbb{F}_q[T]$, where $\mathbb{F}_q$ is a finite field of characteristic p. In this case, some restriction on n is certainly needed, since trivially

$$\gcd(a^{mp^k}-1, b^{mp^k}-1) = \gcd(a^m-1, b^m-1)^{p^k}.$$

In this paper we will show that for $a, b \in \mathbb{F}_q[T]$, even much stronger restrictions on the allowable values of n do not allow one to prove an estimate analogous to (1), much less one as strong as (2).

Acknowledgements. The author would like to thank Gary Walsh for rekindling his interest in arithmetic properties of divisibility sequences and for drawing his attention to the papers [1] and [2], Felipe Voloch for a helpful discussion of Diophantine approximation in characteristic p, and Andrew Granville and the referee for several suggestions that greatly improved this article.

1. A preliminary example

As noted in the introduction, Ailon and Rudnick [1] prove that if $a(T), b(T) \in \mathbb{C}[T]$ are nonconstant polynomials that are multiplicatively independent in $\mathbb{C}(T)$, then

$$\deg\bigl(\gcd(a(T)^n-1, b(T)^n-1)\bigr) \le C(a,b) \qquad \text{for all } n \ge 1.$$

Suppose instead that $a(T), b(T) \in \mathbb{F}_q[T]$, where $\mathbb{F}_q$ is a finite field of characteristic p. It is natural to ask if the Ailon-Rudnick estimate holds, at least if we require that $p \nmid n$. As the following example shows, the answer is no.

Example 1. Let $a(T) = T$ and $b(T) = T+1$, let $Q = p^k$ be some power of p, and take $n = Q-1$. Then

$$\begin{aligned} b(T)^n - 1 = (T+1)^{Q-1} - 1 &= \frac{(T+1)^Q - (T+1)}{T+1} = \frac{(T^Q+1)-(T+1)}{T+1} \\ &= \frac{T^Q - T}{T+1} = \frac{T(T^n-1)}{T+1} = \frac{T(a(T)^n-1)}{T+1}. \end{aligned}$$

Hence

$$\begin{aligned} \gcd(a(T)^n-1, b(T)^n-1) &= \frac{\gcd((T+1)(a(T)^n-1), (T+1)(b(T)^n-1))}{T+1} \\ &= \frac{\gcd((T+1)(a(T)^n-1), T(a(T)^n-1))}{T+1} \\ &= \frac{a(T)^n-1}{T+1}. \end{aligned}$$

Therefore

$$\deg\bigl(\gcd(a(T)^n-1, b(T)^n-1)\bigr) = n-1.$$

2. Basic results on rational function fields over finite fields

Before stating and proving a generalization of the example described in Section 1, we briefly recall some basic arithmetic facts about the rational function field $\mathbb{F}_q(T)$. We start with some notation:

$$\begin{aligned} S_q &= \{\pi \in \mathbb{F}_q[T] : \pi \text{ is monic and irreducible}\}. \\ S_{q,N} &= \{\pi \in S_q : \deg(\pi) = N\}. \\ S_{q,N}(\alpha, \mu) &= \{\pi \in S_{q,N} : \pi \equiv \alpha \pmod{\mu}\}. \end{aligned}$$

$\Phi_q(\mu)$ The function field analog of Euler's function [3, Chapter 1],

$$\Phi_q(\mu) = \#\left(\frac{\mathbb{F}_q[T]}{\mu\mathbb{F}_q[T]}\right)^* = q^{\deg(\mu)} \prod_{\substack{\pi|\mu \\ \pi\in S_q}} \left(1 - \frac{1}{q^{\deg(\pi)}}\right).$$

We are now ready to state three important theorems in the arithmetic theory of (rational) function fields.

Theorem 1 (Prime Number Theorem for Function Fields)**.**

$$\#S_{q,N} = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Proof. See [3, Theorem 2.2] for a proof. To see why this is the analogue of the classical prime number theorem, notice that there are q^N monic polynomials of degree N in $\mathbb{F}_q[T]$, so the fact that $\#S_{q,N}$ is asymptotic to $q^N/\log_q(q^N)$ is analogous to the fact that $\pi(X)$ is asymptotic to $X/\log(X)$. □

Theorem 2 (Primes in Arithmetic Progressions)**.** *Let $\alpha, \mu \in \mathbb{F}_q[T]$ be polynomials with $\gcd(\alpha, \mu) = 1$. Then*

$$\#S_{q,N}(\alpha, \mu) = \frac{1}{\Phi_q(\mu)} \cdot \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right), \tag{3}$$

Proof. See [3, Theorem 4.8] for a proof. Of course, Theorem 1 is the special case of Theorem 2 with $\alpha = 0$ and $\mu = 1$. □

Finally, we will need the following special case of the general r-power reciprocity law in $\mathbb{F}_q[T]$.

Theorem 3 (r-Power Reciprocity)**.** *Let $\pi \in S_q$, let $\mu \in \mathbb{F}_q[T]$, and let r be an odd integer dividing $q - 1$. Then*

$$\pi \equiv 1 \pmod{\mu} \text{ (i.e., } \pi \in S_q(1, \mu)) \Longrightarrow \mu \text{ is an } r^{th} \text{ power modulo } \pi. \tag{4}$$

Proof. Let $\left(\frac{\alpha}{\mu}\right)_r \in \mathbb{F}_q^*$ denote the r^{th} power residue symbol ([3, Chapter 3]), and let $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ be coset representatives for the elements $\alpha \in \mathbb{F}_q[T]/\mu\mathbb{F}_q[T]$ with the property that

$$\left(\frac{\alpha}{\mu}\right)_r = 1.$$

Then one version [3, Proposition 3.6] of the r-power reciprocity law in $\mathbb{F}_q[T]$ says that for any monic irreducible polynomial $\pi \in \mathbb{F}_q[T]$,

$$\pi \equiv \alpha_i \pmod{\mu} \text{ for some } 1 \le i \le t \Longleftrightarrow \mu \text{ is an } r^{\text{th}} \text{ power modulo } \pi.$$

(Note that our assumption that r is odd ensures that either $(q-1)/r$ is even or else $\mathbb{F}_q$ has characteristic 2.) In particular, the implication (4) is an immediate consequence of the fact that $\left(\frac{1}{\mu}\right)_r = 1$ for every modulus μ. □

3. The main theorem

Example 1 shows that for particular polynomials $a(T)$ and $b(T)$, the polynomial $\gcd(a(T)^n-1, b(T)^n-1)$ can be large when $n \equiv -1 \pmod{q}$. We first generalize this example to arbitrary polynomials $a(T)$ and $b(T)$. We then consider more general exponent values and show that it is unlikely that there is any infinite "natural" set of exponents $\mathcal{E}$ with the property that

$$\bigl\{n \in \mathcal{E} : \deg\bigl(\gcd(a(T)^n-1, b(T)^n-1)\bigr) \ge \epsilon n\bigr\}$$

is finite for every $\epsilon > 0$.

Theorem 4. *Let $\mathbb{F}_q$ be a finite field and let $a(T), b(T) \in \mathbb{F}_q[T]$ be nonconstant monic polynomials. Fix any power q^k of q and any congruence class $n_0 \in \mathbb{Z}/q^k\mathbb{Z}$. Then there is a positive constant $c = c(a,b,q^k) > 0$ such that*

$$\deg\bigl(\gcd(a(T)^n-1, b(T)^n-1)\bigr) \ge cn \qquad \text{for infinitely many } n \equiv n_0 \pmod{q^k}.$$

Proof. To illustrate the main ideas, we start with the special case $k = 1$ and $n_0 = -1$, so as in Example 1, we look at exponents n satisfying $n \equiv -1 \pmod{q}$. More precisely, we will take

$$n = q^N - 1 \qquad \text{for } N = 1, 2, 3, \ldots.$$

For all $\pi \in S_{q,N}$, the group $\bigl(\mathbb{F}_q[T]/(\pi)\bigr)^* \cong \mathbb{F}_{q^N}^*$ has order n, so as long as $\pi \nmid ab$, it follows that

$$a^n \equiv b^n \equiv 1 \pmod{\pi}.$$

Hence for all sufficiently large N, e.g. $N \ge \deg(ab)$, we have

$$\gcd(a^n-1, b^n-1) \text{ is divisible by } \prod_{\pi \in S_{q,N}} \pi,$$

and hence

$$\deg\bigl(\gcd(a(T)^n-1, b(T)^n-1)\bigr) \ge \sum_{\pi \in S_{q,N}} \deg(\pi) = (\#S_{q,N}) \cdot N.$$

The "Prime Number Theorem for Polynomials" (Theorem 1) says that

$$\#S_{q,N} = q^N/N + O(q^{N/2}/N),$$

so we find that

$$\deg\bigl(\gcd(a(T)^n-1, b(T)^n-1)\bigr) \ge q^N + O(q^{N/2}) = n + O(\sqrt{n}\,).$$

This completes the proof of the theorem for $n \equiv -1 \pmod{q}$.

In order to obtain more general exponents, we take n to have the form $(q^N-1)/r$ for a suitable choice of N and r. Then $\gcd(a^n-1, b^n-1)$ is divisible by primes π for which both a and b are r^{th} powers modulo π. In order to exploit this weaker condition, we will use the function field versions of the power reciprocity law and Dirichlet's theorem on primes in arithmetic progression.

For now, we assume that $\gcd(q, n_0) = 1$, since this is the most interesting case. At the end of the proof we briefly indicate what to do if n_0 is divisible by the characteristic. Let $r \ge 1$ be the smallest odd integer satisfying

$$r \cdot n_0 \equiv -1 \pmod{q^k},$$

and let

$$Q = q^{k\phi(r)},$$

where $\phi(\,\cdot\,)$ is the usual Euler phi function. We note that

$$Q \equiv 1 \pmod{r}.$$

(If we were aiming for better constants, we could take Q to be any power q^m with $m \ge k$ and $q^m \equiv 1 \pmod{r}$.)

For each power Q^N of Q, we let

$$n = n(Q^N) = \frac{Q^N - 1}{r},$$

and we observe that since $q^k | Q$, we have

$$r \cdot n \equiv -1 \pmod{q^k}, \quad \text{and hence} \quad n \equiv n_0 \pmod{q^k}.$$

It remains to show that $\deg\bigl(\gcd(a(T)^n - 1, b(T)^n - 1)\bigr) \ge cn$ for all $n = n(Q^N)$.

Let

$$\ell(T) = \mathrm{LCM}[a(T), b(T)] \in \mathbb{F}_q[T]$$

be the (monic) least common multiple of $a(T)$ and $b(T)$. We want to use Theorem 3 to find primes for which $a(T)$ and $b(T)$ are r^{th} powers, but in order to apply Theorem 3, we need to work with a sufficiently large base field. More precisely, we work in $\mathbb{F}_Q[T]$, since our choice of Q ensures that the condition $r | Q - 1$ in Theorem 3 is satisfied.

We consider polynomials $\pi \in S_{Q,N}(1, \ell)$, i.e., monic irreducible polynomials of degree N in $\mathbb{F}_Q[T]$ satisfying $\pi \equiv 1 \pmod{\ell}$. Then

$$\begin{aligned}
\pi \in S_{Q,N}(1,\ell) &\Longrightarrow \pi \equiv 1 \pmod{a} \quad \text{and} \quad \pi \equiv 1 \pmod{b} \\
&\Longrightarrow a \equiv A^r \pmod{\pi} \quad \text{and} \quad b \equiv B^r \pmod{\pi} \\
&\qquad\qquad \text{for some } A, B \in \mathbb{F}_Q[T], \text{ from Theorem 3,} \\
&\Longrightarrow a^n \equiv (A^r)^{(Q^N-1)/r} = A^{Q^N-1} \equiv 1 \pmod{\pi} \quad \text{since } \deg \pi = N, \\
&\qquad\qquad \text{and similarly } b^n \equiv 1 \pmod{\pi}.
\end{aligned}$$

This proves that $\gcd(a(T)^n - 1, b(T)^n - 1)$ is divisible by every polynomial in $S_{Q,N}(1, \ell)$, so we obtain the lower bound

$$\begin{aligned}
\deg\bigl(\gcd(a(T)^n - 1, b(T)^n - 1)\bigr) &\ge \sum_{\pi \in S_{Q,N}(1,\ell)} \deg(\pi) \\
&= \#S_{Q,N}(1,\ell) \cdot N \\
&= \frac{Q^N}{\Phi_Q(\ell)} + O(Q^{N/2}) \qquad \text{from Theorem 2,}
\end{aligned}$$

where recall that

$$\Phi_Q(\ell) = \#\left(\frac{\mathbb{F}_Q[T]}{\ell \mathbb{F}_Q[T]}\right)^* = Q^{\deg(\ell)} \prod_{\substack{\pi \mid \ell \\ \pi \in \mathcal{S}_Q}} \left(1 - \frac{1}{Q^{\deg(\pi)}}\right).$$

Finally, using the definition $n = (Q^N - 1)/r$, we see that

$$\deg\bigl(\gcd(a(T)^n - 1, b(T)^n - 1)\bigr) \ge \frac{r}{\Phi_Q(\ell)} \cdot n + O(\sqrt{n})$$

$$\text{for all } n = \frac{Q^N - 1}{r},$$

where the big-O constant is independent of N. This gives the desired result, with an explicit value for c.

We are left to deal with the case that n_0 is divisible by the characteristic p of $\mathbb{F}_q$. Write $n_0 = p^i \cdot n_1$ with $p \nmid n_1$. From the result proven above, we know that

$$\deg\bigl(\gcd(a(T)^n - 1, b(T)^n - 1)\bigr) \ge cn \quad \text{for infinitely many } n \equiv n_1 \pmod{q^k}. \tag{5}$$

For these values of n, it follows

$$\begin{aligned}\deg\bigl(\gcd(a(T)^{p^i n} - 1, b(T)^{p^i n} - 1)\bigr) &= \deg\bigl(\gcd((a(T)^n - 1)^{p^i}, (b(T)^n - 1)^{p^i})\bigr)\\ &= p^i \deg\bigl(\gcd(a(T)^n - 1, b(T)^n - 1)\bigr)\\ &\ge cp^i n\end{aligned}$$

and that

$$p^i n \equiv p^i n_1 = n_0 \pmod{q^k}.$$

Thus the values $p^i n$ with n satisfying (5) show that Theorem 4 is true when $p|n_0$. □

Remark 1. The proof of Theorem 4 shows that it is true for any

$$c < \frac{1}{\Phi_Q(\mathrm{LCM}[a(T), b(T)])},$$

where Q is a certain explicit, but potentially quite large, power of q. More precisely, we can take $Q = q^m$ for some $m < 2kq^k$, but this huge number is undoubtedly far from optimal.

Remark 2. We conclude this note by again displaying the striking "trichotomy" in the values of $\gcd(a^n - 1, b^n - 1)$:

$$\begin{aligned}\mathbb{Z}: &\qquad \log\bigl(\gcd(a^n - 1, b^n - 1)\bigr) \le \epsilon n.\\ \mathbb{F}_q[T]: &\qquad \deg\bigl(\gcd(a^n - 1, b^n - 1)\bigr) \ge cn.\\ \mathbb{C}[T]: &\qquad \deg\bigl(\gcd(a^n - 1, b^n - 1)\bigr) \le c.\end{aligned}$$

For $\mathbb{F}_q[T]$ and $\mathbb{C}[T]$, these estimates are best possible, aside from the delicate question of the value of the constants. However, the situation for $\mathbb{Z}$ is less clear. Bugeaud, Corvaja, and Zannier [2, Remark 2 after Theorem 1] note that there is an absolute constant $c = c(a, b) > 0$ so that

$$\log\bigl(\gcd(a^n - 1, b^n - 1)\bigr) \ge \frac{cn}{\log\log n}$$

holds for infinitely many n. It is reasonable to guess that this lower bound is also an upper bound, with an appropriate larger choice of c. However, it appears to be an extremely difficult problem to prove any upper bound of the form

$$\log\bigl(\gcd(a^n - 1, b^n - 1)\bigr) \le f(n)$$

with $f(n)$ satisfying $f(n)/n \to 0$.

References

[1] N. Ailon, Z. Rudnick, Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$, *Acta Arithmetica*, <http://arxiv.org/abs/math.NT/0202102>, to appear.

[2] Y. Bugeaud, P. Corvaja, U. Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, *Math. Zeit.* **243** (2003), no. 1, 79–84.

[3] M. Rosen, *Number theory in function fields*, GTM 210, Springer-Verlag, New York, 2002.

[4] W. Schmidt, *Diophantine approximation*, Lecture Notes in Mathematics 785, Springer-Verlag, Berlin, 1980.

Mathematics Department, Box 1917, Brown University, Providence, RI 02912 USA
jhs@math.brown.edu